TRUSTED
COMPUTER SOLUTIONS

SecureOffice® Trusted Workstation™ Administrator Training

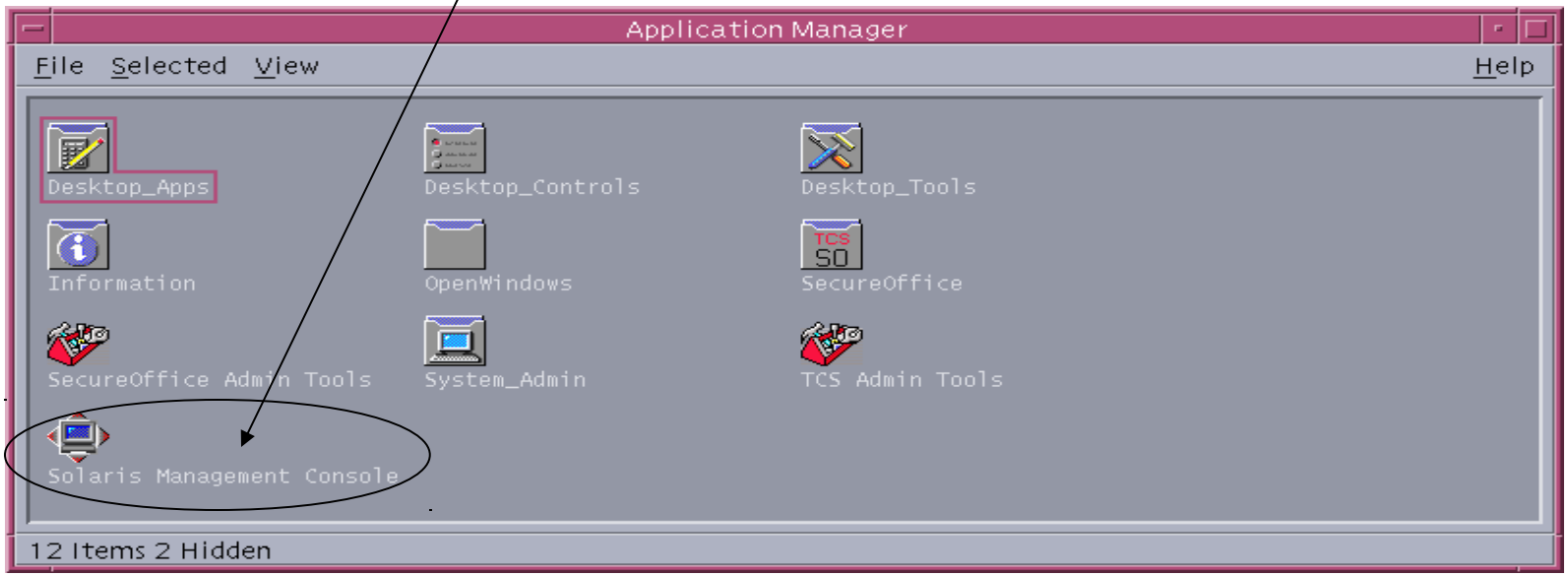
Module Four: System Administration Tasks

Trusted Computer Solutions, Inc.
2350 Park Center Drive, Suite 500
Herndon, VA 20171 USA
+1.703.318.7134 (Phone)
+1.703.318.5041 (Fax)
www.TrustedCS.com

SecureOffice® Trusted Workstation™ (TWS) Administrator

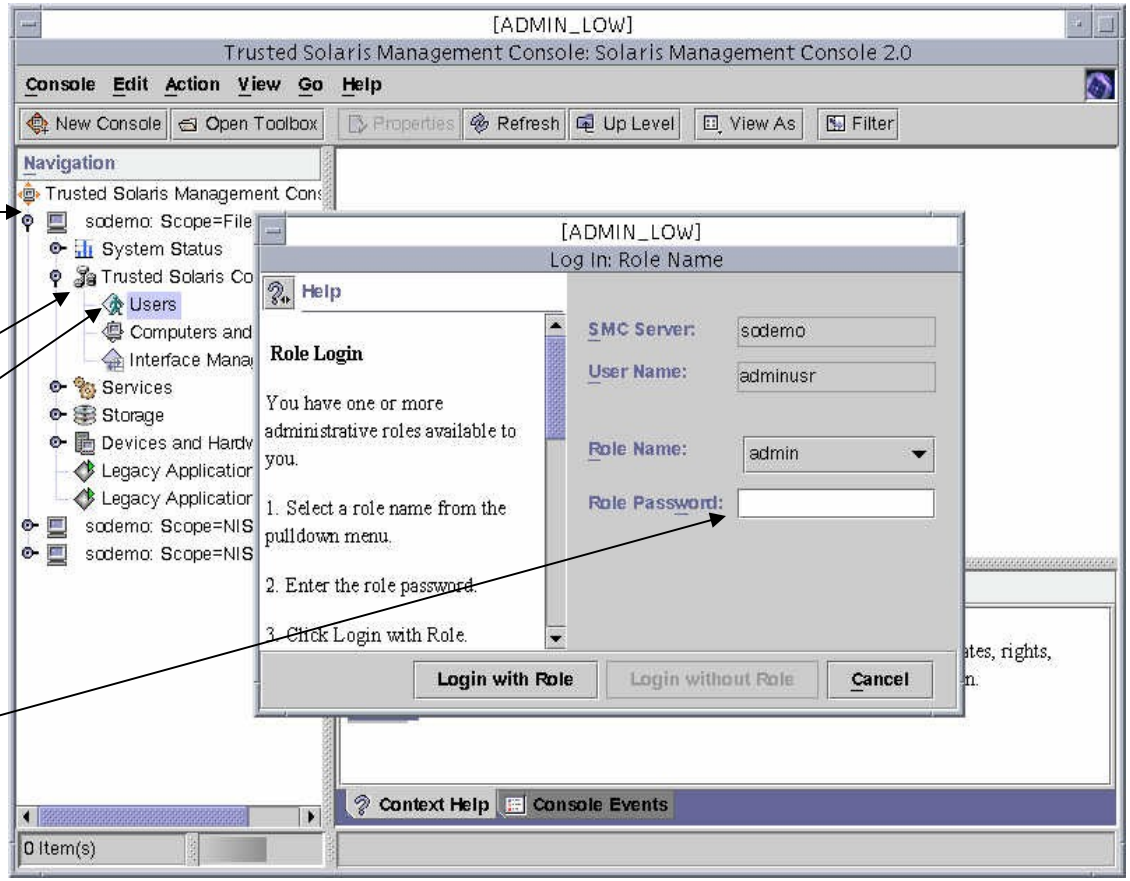
- System Administration Tasks
  - Solaris Management Console
    - Account Management
  - Backup and Recovery Management
  - Audit Management
  - Electronic Mail Management
  - Printer Configuration Management
  - IP Packet Filtering Management
  - VFind Virus Scan Management
  - Citrix Client Management

- Launching Solaris Management Console
  - First assume an administration role in which to run SMC
    - admin role or secadmin role
  - Launch Application Manager
  - Left double-click on SMC icon to run SMC application



Launching Solaris Management Console (con't)

- Select **Scope** type relevant to site configuration
  - Files
  - NIS+
  - NIS
- Select **Trusted Solaris Configuration**
- Select Appropriate sub menu tool set
  - Users
- Requests login as role to proceed further.

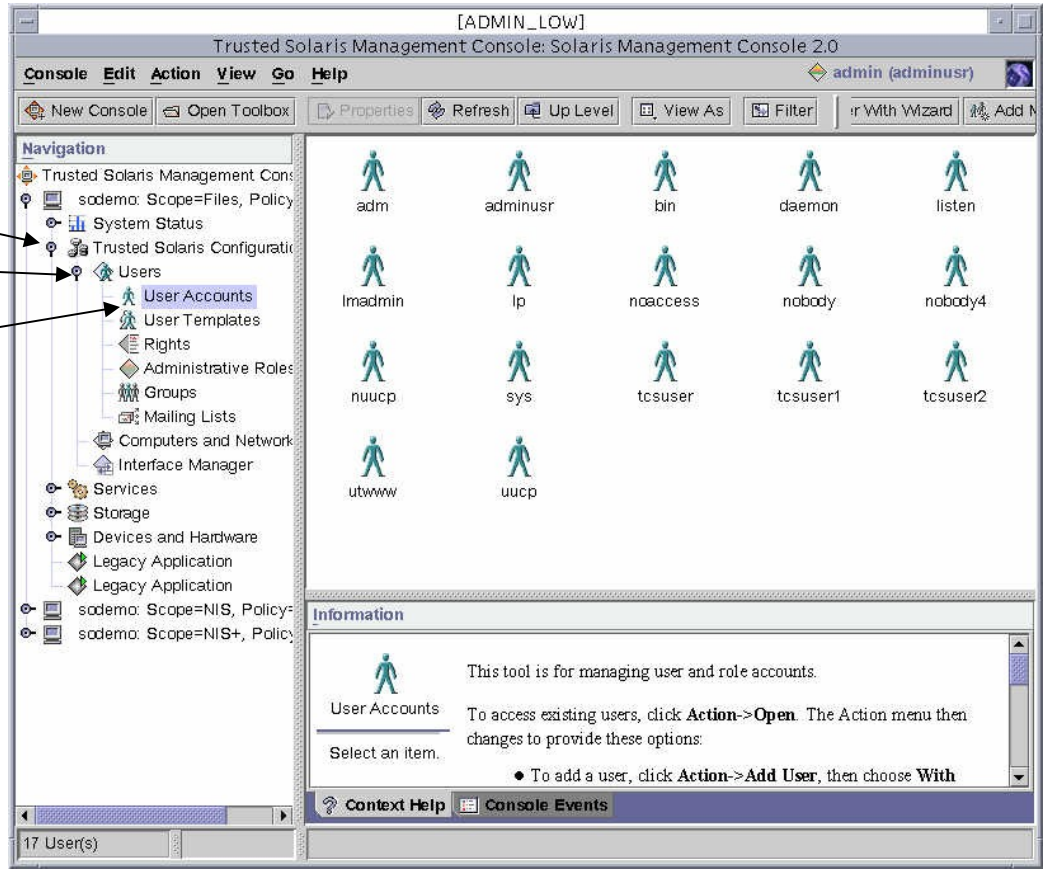


- User Account Management
  - Adding Accounts
  - Modifying Accounts
  - Deleting Accounts
  - Unlocking a Locked Account

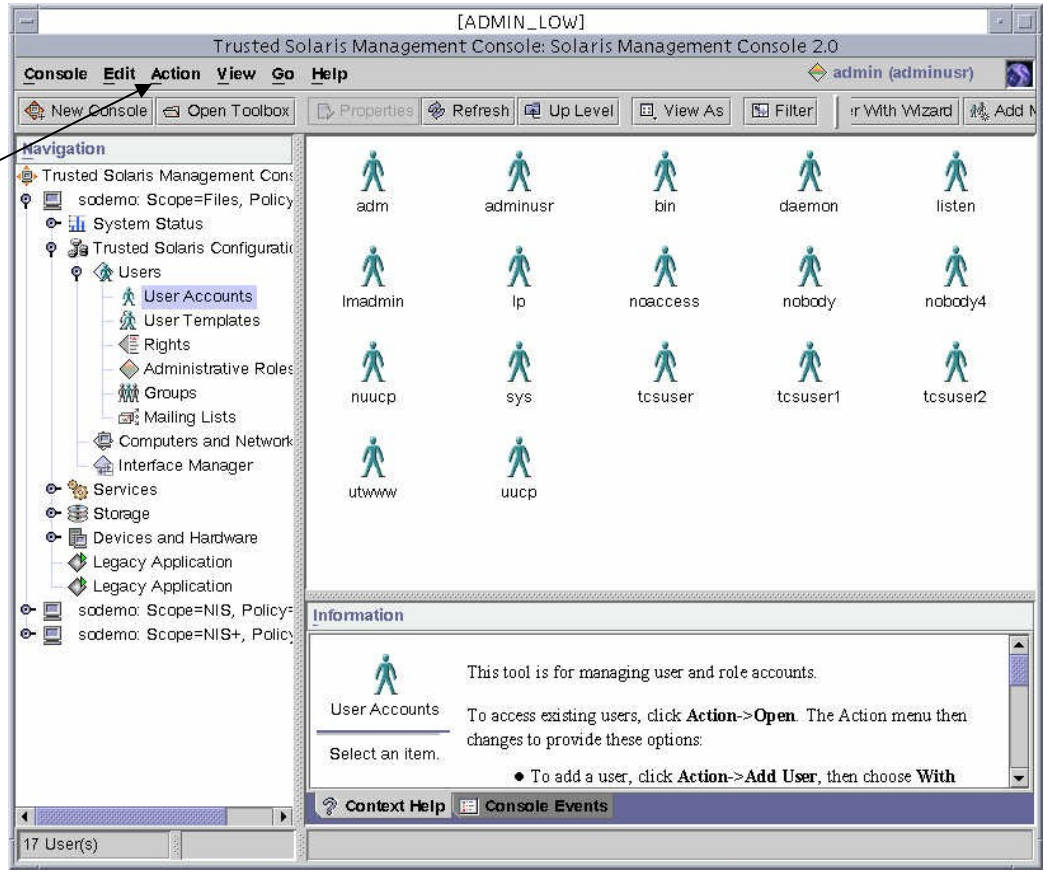
- Adding Accounts
  - The `admin` role must first set up each new user account and assign its non-security relevant account attributes.
  - The `secadmin` role then specifies the account's security-relevant attributes and activates the account.

- Adding Accounts (con't)
  - Assume the admin role and launch the Application Manager.
  - Click on the **Solaris Management Console** icon to launch the Solaris Management Console tool
  - For Non-NIS+ configurations "Files"
    - Under the Navigation column, select <hostname>: Scope=Files, Policy=TSOL → Trusted Solaris Configuration → Users.
  - For NIS+ configurations
    - Under the Navigation column, select <hostname>: Scope=NIS+, Policy=TSOL → Trusted Solaris Configuration → Users

- Adding Accounts (con't)
  - Select **Trusted Solaris Configuration**
  - Select **Users**
  - Select **User Accounts**

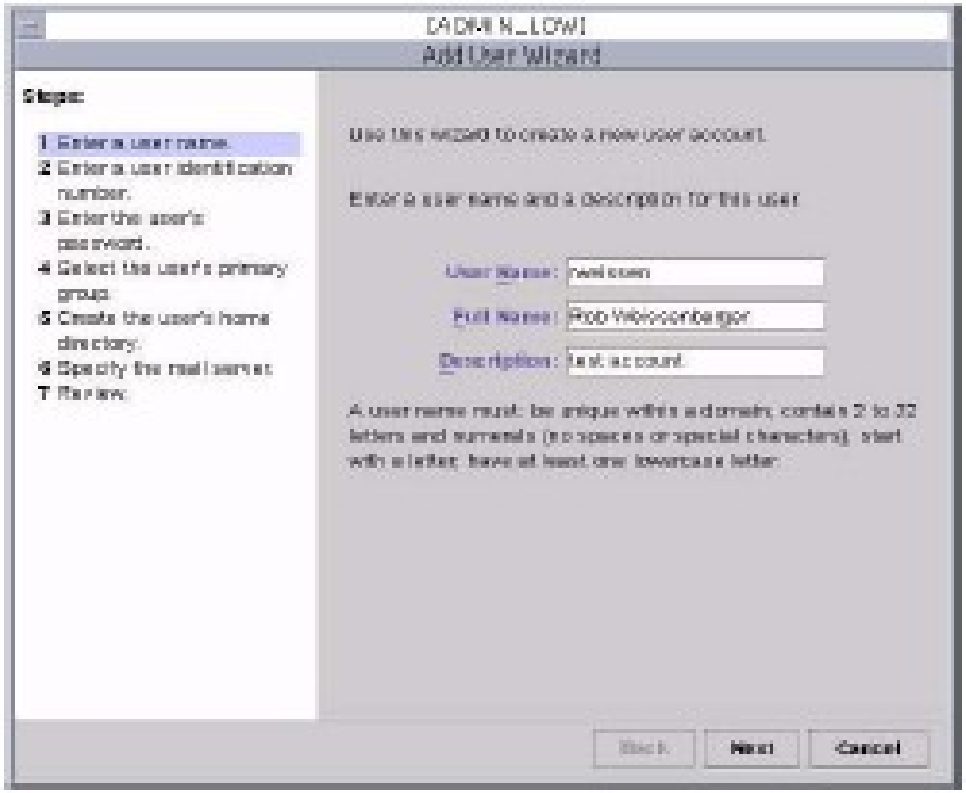


- Adding Accounts (con't)
  - **Users → User Accounts**
    - From menu bar, select **Action → Add User → With Wizard** to launch the Add User Wizard tool



Adding Accounts (con't)

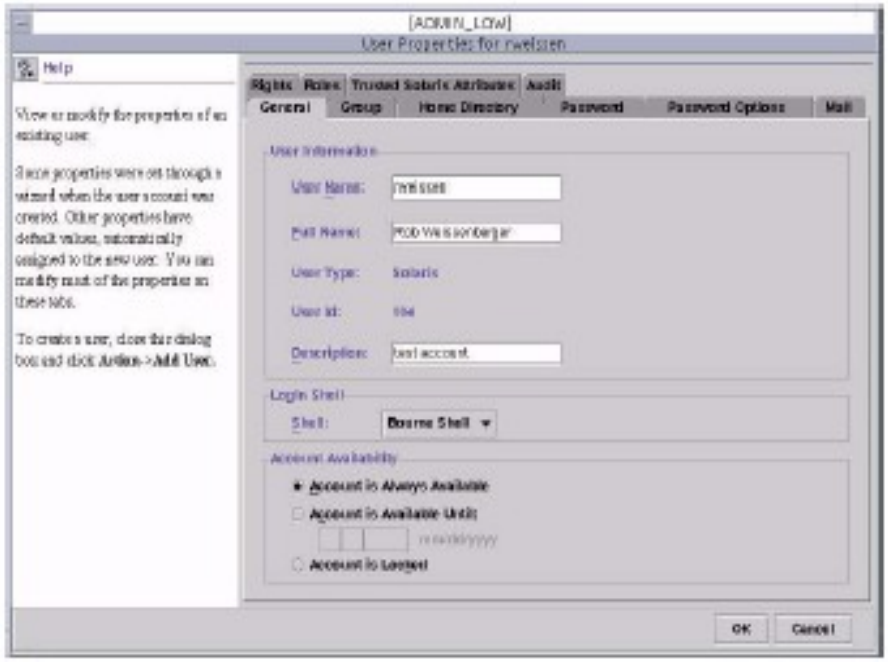
Add User Wizard



- User Account Management
  - Adding Accounts
    - Enter the `User Name`, `Full Name`, and `Description`, and click `Next`.
    - Enter the `User ID Number`, and click `Next`.
    - In the drop-down menu next to `Set Password By`
      - » select either `Type In` or `Choose From List`.
      - » Assign a password, and click `Next`.
    - Select a group in the drop-down menu next to `Primary Group`, and click `Next`.
    - Enter the user's home directory in the `Path` box, and click `Next`.
    - Enter the mail server, and click `Next`.
    - Review the user account information and click `Finish` to complete the actions required by the `admin` role for creating a new account.

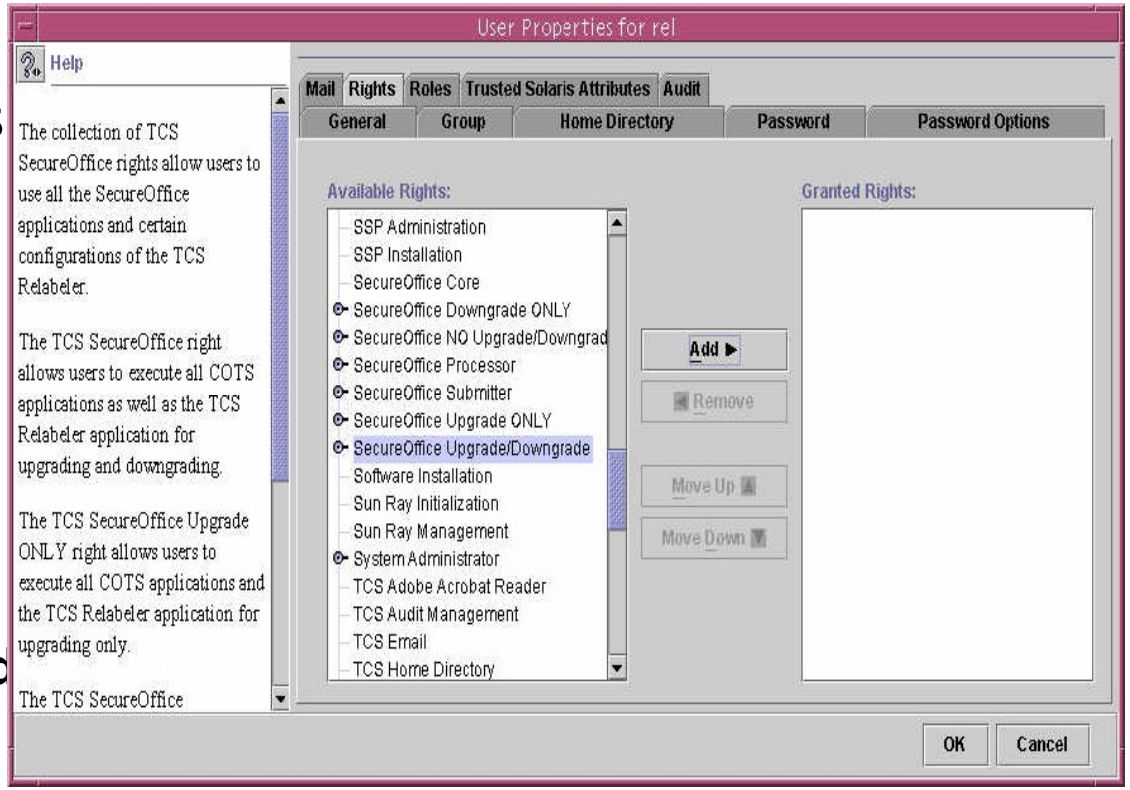
- Adding Accounts (con't)
  - Assume the secadmin role and launch the Solaris Management Console tool.
    - For Non-NIS+ configurations
      - » Under the Navigation column, select <hostname>: Scope=Files, Policy=TSOL → Trusted Solaris Configuration → Users.
    - For NIS+ configurations
      - » Under the Navigation column, select <hostname>: Scope=Files, Policy=TSOL → Trusted Solaris Configuration → Users.
    - Type in the password for secadmin when prompted, and press <CR>.
    - Select the account to be activated. With the User Accounts sub-option highlighted under Users, double-click on the newly created account to launch the User Properties tool.

- Adding Accounts (con't)
  - User properties tool
  - Assign user rights as follows:
    - Click on the Rights tab at the top of the User Properties tool to launch the User Rights window



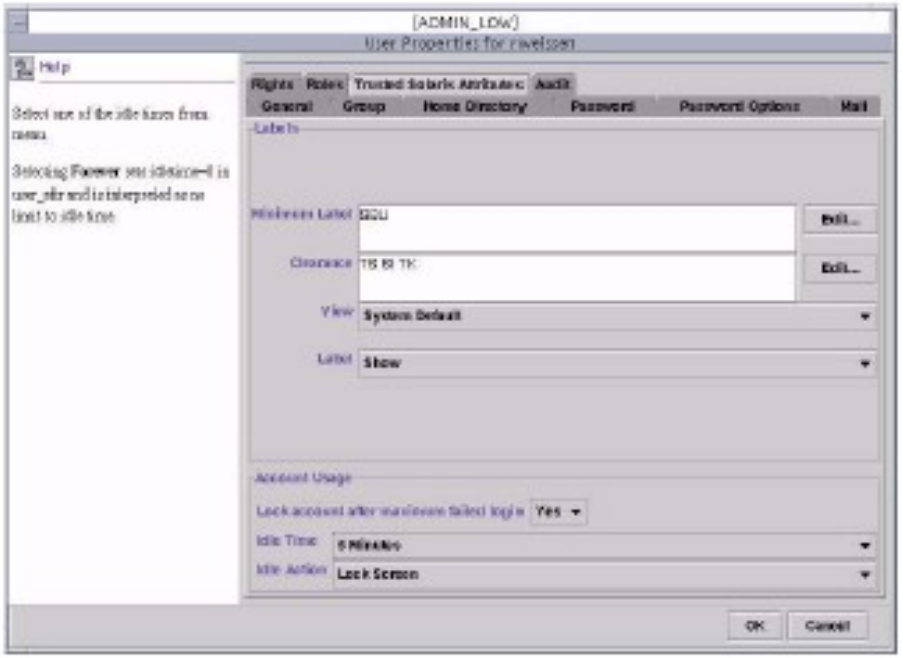
Adding Accounts (con't)

- Assign user rights as follows:
  - Highlight the appropriate ***SecureOffice*** right in the **Available Rights** column
  - Click the **Add** button to add this right to the **Granted Rights** column.

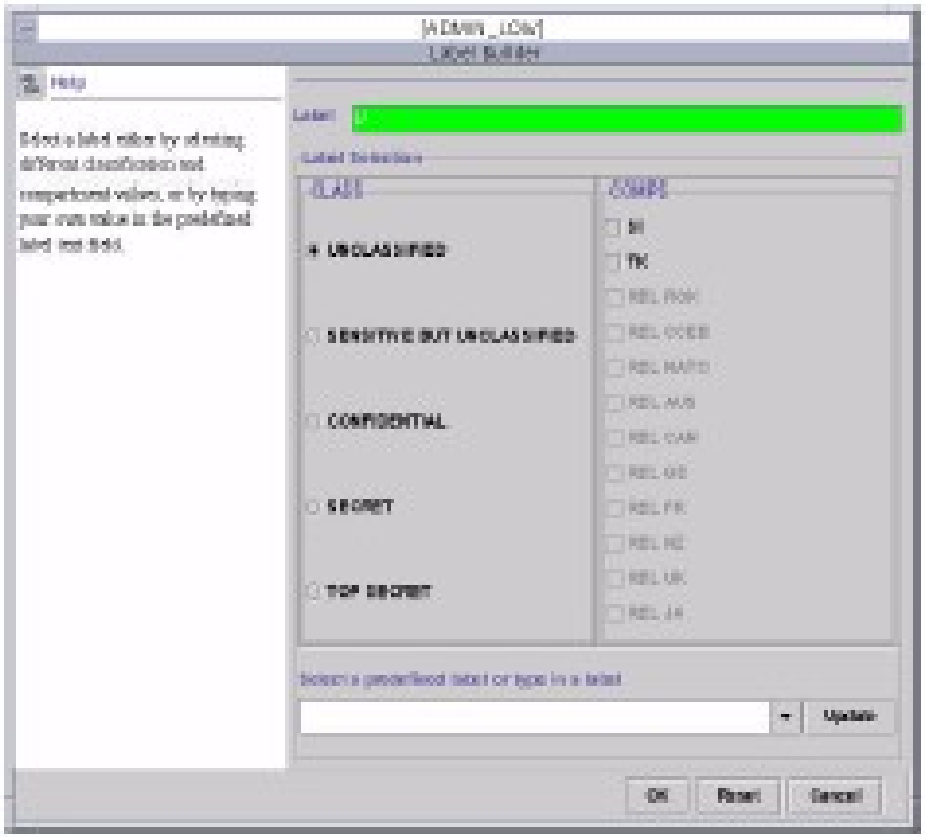


- Adding Accounts (con't)
  - User Profile (a.k.a "Rights") Considerations
    - SecureOffice Core
    - SecureOffice NO Upgrade/Downgrade
    - SecureOffice Submitter
    - SecureOffice Processor
    - SecureOffice Downgrade ONLY
    - SecureOffice Upgrade ONLY
    - SecureOffice Upgrade/Downgrade

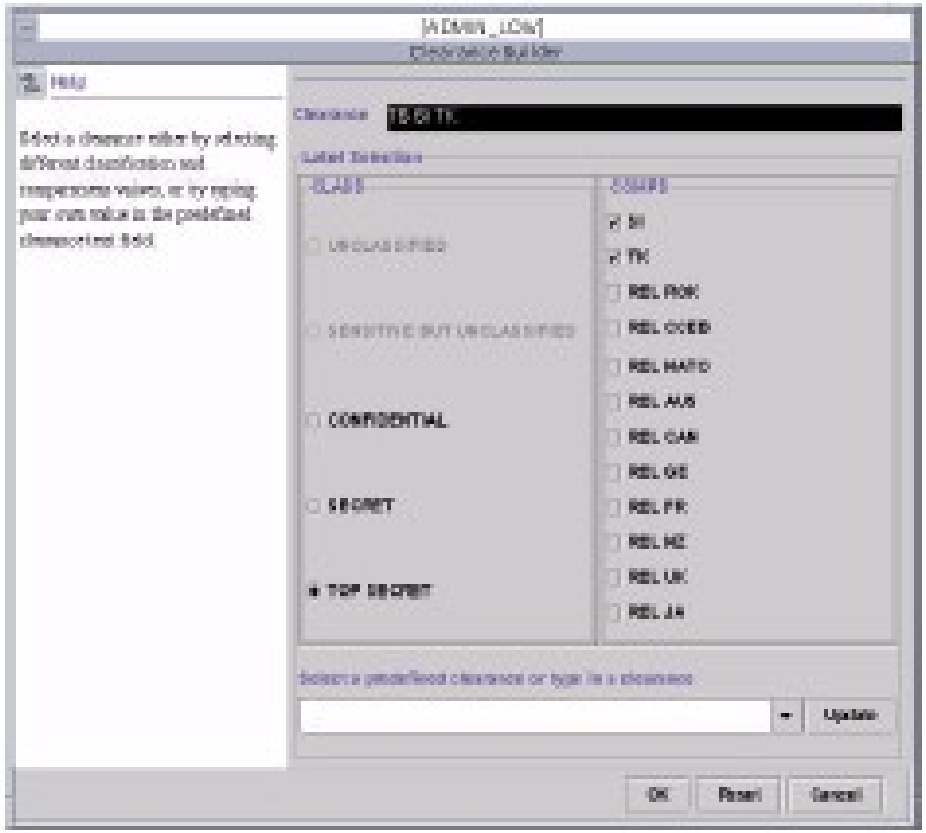
- Adding Accounts (con't)
  - Click **Trusted Solaris Attributes** tab to launch **Trusted Solaris Attributes** window.
  - Set the **Idle Time** and **Idle Action** attributes, if necessary.



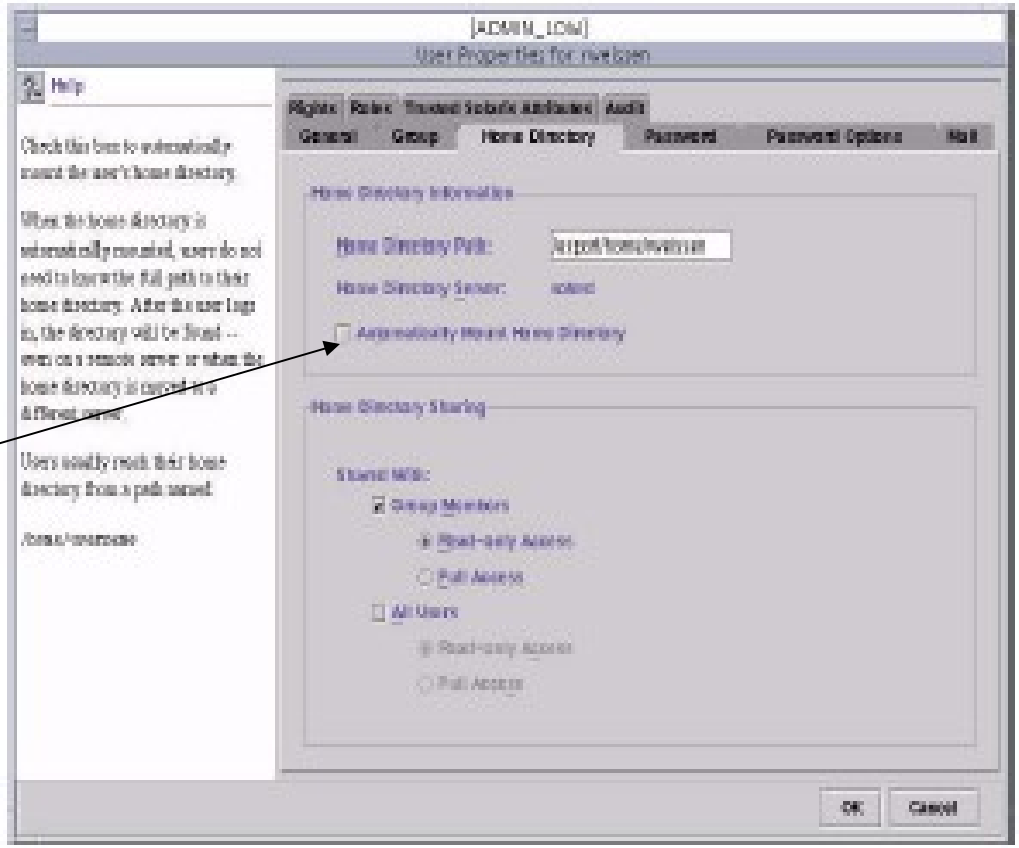
- Adding Accounts (con't)
  - Click **Edit** button to the right of the **Minimum Label** to launch the **Label Builder** tool
    - Assign the appropriate minimum SL, and click **OK**.



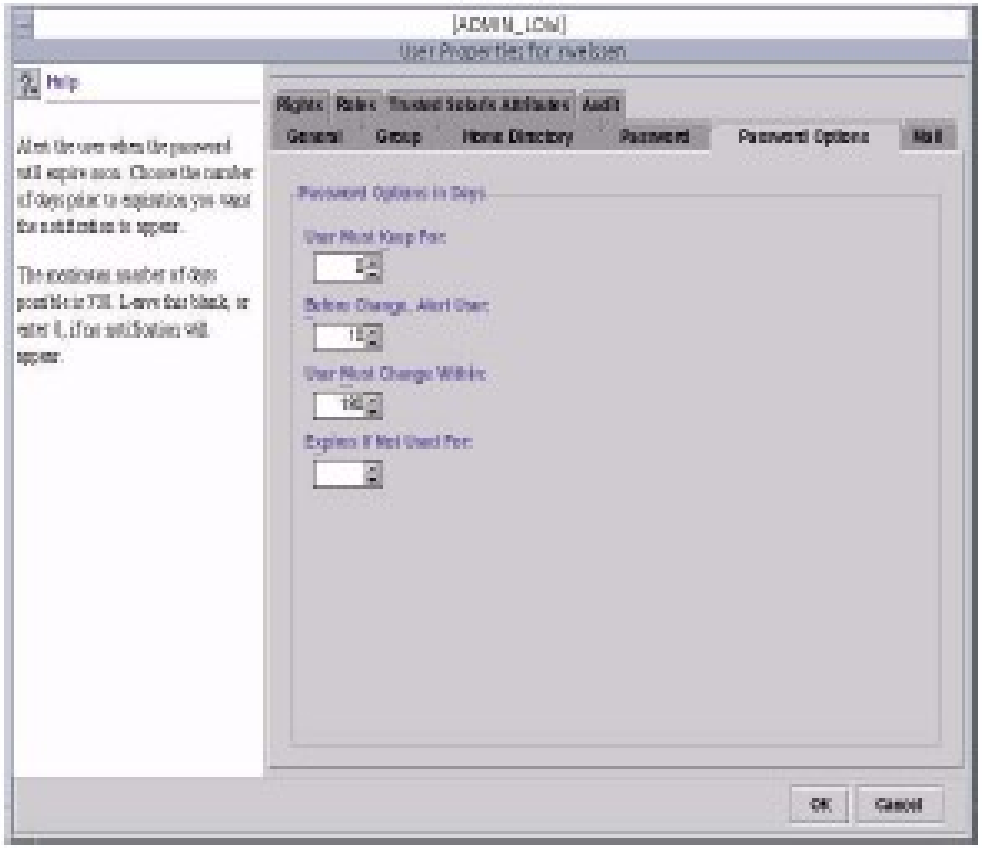
- Adding Accounts (con't)
  - Click Edit button to the right of the Clearance box to launch the Clearance Builder tool
    - Assign the appropriate SL, and click OK.
    - Typically, the highest SL available should be assigned as account's clearance.



- Adding Accounts (con't)
  - Assign home directory attributes as follows:
    - Click on the **Home Directory** tab to launch the **Home Directory** window
      - » Uncheck the **Automatically Mount Home Directories** option.



- Adding Accounts (con't)
  - Assign password attributes
    - Click **Password Options** tab to launch the **Password Options** window.



- Adding Accounts (con't)
  - Default password change values
    - Required satisfy system accreditation.
  - Activate the account.
    - Table summarizes the attribute settings that should be established for accounts.
  - Click on OK in the User Properties tool to save changes to disk and activate the account.
  - Click Cancel to abort the account creation.

Attribute	Value
User Must Keep For	0 days
User Must Change Within	180 days
Before Change, Alert User	10 days
Expires If Not Used For	(Leave Blank)

- Adding Accounts (con't)
  - Table summarizes the attribute settings that should be established for accounts.
  - Activate the account.
    - Click on **OK** in the User Properties tool to save changes and activate the account.
    - Click **Cancel** to abort the account creation, if necessary.

Parameter	Regular User Setting	Administrative User Setting
Primary Group	10	10
Supplementary Groups	none	none
Home Path	/export/home/<account>	/export/home/<account>
Login Shell	/bin/sh	/bin/sh
Clearance	highest available to users	highest available to users
Minimum SL	SBU	SBU
Password must Keep For	0 days	0 days
Password must Change within	180 days	180 days
Alert User Before Password Change	10 days	10 days
Roles	<none>	admin,secadmin and/or root
Profiles	SecureOffice User Profile or SecureOffice User Profile (no upgrade/downgrade)	SecureOffice User Profile or SecureOffice User Profile (no upgrade/downgrade)

- Modification of Accounts
  - Modification of attributes are restricted in similar fashion as adding account
  - Requires secadmin and/or admin roles
  - Uses the same interface for all account administration actions

- Deleting Accounts
  - Before a user account is deleted and if required, the secadmin role should identify all of the files owned by the user and transfer ownership of the files to an appropriate account.
    - Assume the secadmin role at ADMIN_HIGH and launch a Terminal window.
    - Identify all files owned by the account by typing:
      - » $ **find / -M -user *userid* -print**
      - » Move all identified files to an appropriate account
  - After the secadmin role has transferred file ownership to an appropriate account, the admin role deletes the account's home directory, deletes the account's mail entries box, and deletes the account.

- Deleting Accounts
  - Assume admin role and launch Solaris Management Console tool
    - Highlight the account designated for deletion and select Edit → Delete.
    - Delete the account's home directory and mail entries box.
      - » In the pop-up window, highlight the **Delete User's Home Directory** and **Delete User's Mail Entries** boxes and click **OK**.
      - » Confirm the deletion by clicking **Yes** on the deletion confirmation screen.

- Unlocking Accounts
  - Access account in same manner as adding account
  - Three unsuccessful login attempts will lock an account
    - Do not attempt to log into the system as root -- you may lock role
  - Recovery of locked account
    - Assume the **secadmin** role and launch **Solaris Management Console** tool
    - Double-click account name to unlock, or select **Action Properties**
    - Select **Account is Always Available** or **Account is Available Until MMDDYY** radio button
  - Assign a temporary password to the account.
    - Click on the down-arrow next to **Password** and select **Type in**.
    - In pop-up window, enter and confirm a temporary password, then click **OK**.
    - Click **OK** in the **Password** window
    - Click **Done** in the **User Manager**: **Navigator** tool
    - Click **Exit** in the **User Manager** tool.

- Backup and Recovery
  - Performing regular system backups
    - Configuration file backups
    - Command line backups
    - ‘cron’ job execution
  - Backup logs
  - Performing a system restore
  - Emergency Recovery
    - Recovering an entire system

- Backup and Recovery
  - Performing regular system backups
    - /usr/local/admin/tcs_dump program provides a robust backup solution
      - » Online backups
      - » Configuration file to specify which file systems are backed up when
      - » SCSI autoloader support
      - » Detailed logging
    - Administrator can manually dump a single partition to tape
    - ufsdump command available to admin and root roles

- Backup and Recovery
  - Using the configuration file for backups
  - Must be run as root role at ADMIN_HIGH
  - Run backup with command : /usr/local/admin/tcs_dump -r
    - Based on day of the week
    - Specify ufsdump level, backup tape device, file systems to be backed up

```
#
# Config file for TCS backup script
# Day-of-Week:tape device:dump-level:tape-number:append-to-existing-archive:eject:verify:partitions:
#
# Day-of-Week: Each day that you want save action taken
#              Must be a valid 3 character abbreviation for day of week as used by date command
#              REQUIRED, NO DUPLICATES
# tape device: valid device in the /dev/rmt directory - REQUIRED
# dump-level:  valid dump level as used by ufsdump (0-9) - REQUIRED
# tape-number: tape slot in the autoloader magazine, 1-32 - OPTIONAL
# append-to-existing-archive: an "a" if you want archive append to tape number - OPTIONAL
# eject: an "e" if you want to eject the tape or magazine - OPTIONAL
# verify:  *Reserved for future use
# partitions: a space separated list of paritions to save - REQUIRED
# Example:
# Mon:0m:2:3::::/ /opt /var /usr:
#
Sun:0m:0:1::::/ /opt /usr /var /data:
Mon:0m:5:3::::/ /opt /usr /var /data:
Tue:0m:5:3::::/ /opt /usr /var /data:
Wed:0m:5:4::::/ /opt /usr /var /data:
Thu:0m:5:4:a::::/ /opt /usr /var /data:
Fri:0m:5:5::::/ /opt /usr /var /data:
Sat:0m:5:5:a:e::/ /opt /usr /var /data:
```

- Backup and Recovery
  - Using the command line for one-time backups
    - Help file : /usr/local/admin/tcs_dump –h
    - Same options available
    - Example :
      - » /usr/local/admin/tcs_dump –l 5 –f 0m –A 6 –a –e / /opt
      - » Writes backup at ufsdump level 5 to slot 6 in an autoloader device of the / and /opt filesystems.

- Backup and Recovery
  - Setting up ‘cron’ jobs allows backups to be run in off-peak hours
    - All ‘cron’ modifications must be done as the root role at ADMIN_HIGH
    - Edit both configuration file (tcs_dump.config) and crontab
    - Example below assumes setup shown in Configuration file example
      - » Backup will run each night of the week at 1am and reads the Configuration file for parameters.

```
Crontab file :
0 1 * * 0-6 /usr/local/admin/tcs_dump -r
```

- Backup and Recovery
  - Backup Logs
    - All logs are created at ADMIN_HIGH
    - Creates a date/time stamped log for each backup
    - Located in /etc/security/tcs/logs/tcs_dump.mmddyyHHMMSS

- Backup and Recovery
  - Performing a system restore
    - Restoring Select Files, Directories, or File Systems
      - » ufsrestore command allows for selective file recovery
    - Restoring an entire partition
      - » Warning: This method is destructive to partition contents
      - » ufsrestore can restore a single partition from the tape created with exadump
      - » See the Administrator's Guide for more info

- Audit Management

  ***Note**: This function is available using the Audit Reduction Tool discussed in Module 2.*

  - Necessary Files/Directories
  - System-Level Auditing
  - User-Level Auditing
  - Audit Reduction Tools
  - Switching Audit Collection Files
  - Compressing Audit Collection Files
  - Cleaning up not_terminated Audit Collection Files
  - Audit Trail Overflow
  - NIS+ Master/Client Considerations

- Necessary Files/Directories
  - `/etc/security/audit_event` – Specifies the auditable events on the workstation. This file should not be modified; the system accreditation may be invalidated if file is changed.
  - `/etc/security/audit_class` – Specifies the audit class definitions on the workstation. This file should not be modified; the system accreditation may be invalidated if the file is changed.
  - `/etc/security/audit_startup` – This file's existence causes the audit daemon to run automatically in multi-user mode. This file is an executable script that is invoked as part of the boot sequence.
  - `/etc/security/audit_control` – Specifies the audit directory location (i.e., `/etc/security/audit/`*`systemname`*`/files`), the threshold for the minimum free-space on the audit file system (i.e. minfree, with a default of 20 percent), and the list of enabled audit classes on the workstation (i.e., flags).

- Necessary Files/Directories (con't)
  - `/var/audit` - local system directory that contains audit data. `/etc/security/audit/localhost/files` is a link to this directory.
  - `/var/audit/compressed_trails` - directory used to compress/terminate audit data.
  - Audit Data File Format - `/var/audit/XXX.YYY.hostname` - XXX is start time, YYY is end time and hostname is hostname of system. `YYY.not_terminated` indicates current audit or not properly terminated audit trail.

- System-Level Auditing
  - An audit class is a set of predefined audit events that have been grouped together.
  - The flags line of the `/etc/security/audit_control` file specifies the enabled audit classes that are audited for all users on the machine.
  - These audit classes are referred to as the machine-wide audit flags or the machine-wide audit pre-selection mask.

- User-Level Auditing
  - If it is desirable to audit some users and roles differently from others, `secadmin` may edit the `/etc/security/audit_user` file to add audit flags for individual users and roles.
  - The **audit_user** flags combine with the **system-wide** flags specified in the `/etc/security/audit_control` file to determine which classes of events to audit for that user or role.

- Audit Reduction Tools
  - Audit records are useful only if they are reviewed regularly for anomalous activity.
  - Root role can run **auditreduce** and **praudit** at **ADMIN_HIGH** only
    - **auditreduce** - merges audit collection files and allows **root** role to choose appropriate sets of records to examine.
    - **praudit** - prints the audit records (which are stored in a format that is not human-readable) in a human-readable form that allows **root** role to review the audit records in an interactive display, to create reports, and to maintain statistics.
    - **tcs_auditb** - places a separator between audit records to enhance readability

- Switching Audit Collection Files
  - To keep audit files at a manageable size, it is necessary to routinely switch audit collection files
  - The interval will be determined by the amount of activity on the workstation and the audit class configuration
  - Switching audit collection files is performed by **secadmin** role at **ADMIN_HIGH** with the command:
    - # audit –n
  - TCS recommends using a cron job to perform this function at least daily. This should be done as **secadmin** at **ADMIN_HIGH**
    - 1 0 * * * * /usr/local/sbin/audit -n

- Compressing Audit Collection Files
  - Audit collection files can become quite large, consuming a significant percentage of secondary storage.
  - A file compression utility is provided to reduce the size of a file to approximately one-tenth of its original size.
  - The **compress_audit** utility examines the **/var/audit** directory, takes all but the current audit file, and compresses those files in **/var/audit/compressed_trails**.
  - **compress_audit** is executed based on an entry in the system crontab file.
    - 5 0 * * * /etc/security/tcs/scripts/compress_audit

    ***Note: This should be done in conjunction with rotating the audit logs (previous slide)*

- Cleaning up Collection Files
  - Occasionally, if a system terminates abnormally while its audit collection file is still open, the end time of that file remains a string "`not_terminated`" even though the file is no longer being used to write audit records.
  - When such a file is found, root can manually verify that the file is no longer in use and properly terminate the file.
  - Terminate file by first moving it to the `compressed_trails` directory **ADMIN_HIGH**.
  - Execute the command "`auditreduce -O` *`hostname audit_trail`*" where *`hostname`* is the hostname of system and *`audit_trail`* is the unterminated audit trail filename in file format *XXX*`.not_terminated.hostname` where *XXX* is audit start date.

- Audit Trail Overflow
  - If the audit file system containing the current audit collection file reaches the `minfree` threshold configured in `audit_control`, the `audit_warn` script sends a message to the console and to the `audit_warn` mail alias that the threshold has been exceeded on the audit file system.
  - To prevent audit trail overflow, use the following instructions
  - Establish a schedule for regularly compressing audit collection files, archiving them to tape, and deleting the compressed audit collection files from the audit file.
  - If the **audit_warn** script sends a warning message about minfree being reached, it is essential that there be prompt response to provide space for placing more audit data in the audit file system(s).

- Audit Trail Overflow (con't)
  - If the audit file system becomes full, no user (including administrative users) will be able to log in to the workstation.
  - To recover from a full audit file system, an administrator who knows the PROM password will have to boot the system into single-user mode and repair the audit trail by hand.
  - Call TCS to walk you through the recovery if you have this problem.

- NIS+ Master/Client Considerations
  - In a NIS+ Master/Client configuration it is possible to export the audit data from all of the NIS+ Clients to the NIS+ Master Server.
  - This allows for centralized administration of audit of all systems from the NIS+ Master Server

- Electronic Mail Management
  - Receiving Mail via Remote Servers
  - Receiving Mail via Local SMTP
  - Sending Mail

- Receiving Mail via Remote Server
  - Mail is stored on a remote server until retrieved by a program on user's behalf
  - Protocols used: POP2/POP3, IMAP
    - Is the preferred method of mail retrieval
    - Allows for the only "available" incoming service to be filtered out (SMTP)
    - Requires applications like Netscape or Applix for mail retrieval
    - These applications must be configured by each user

- Receiving Mail via Local SMTP
  - Mail is stored on workstation and is available when user logs in
    - Requires administrator knowledge of `sendmail.cf` to setup and/or administer
    - `sendmail.cf` stored in a Multi-Level Directory (MLD)
      - » Separate sendmail.cf for each level allows different configurations for each network.
    - `sendmail` is run out of `inetd` not in daemon mode
  - Protocol used: SMTP
    - Requires SMTP be made an “available” incoming service. By default this service is not filtered on incoming requests.
    - Can use applications like Netscape, Applix, or Sun provided DTMail program.
      - » Applications must be configured by each user

- Sending Mail
  - Protocol used SMTP
  - Is the internet standard for mail delivery
  - Almost all Mail User Agent (MTA) applications like Netscape, Applix, or Sun provided DTMail program use SMTP to send mail
    - Can configure MTA to use local machine sendmail or external remote SMTP server for mail delivery.
    - If using local machine, “localhost” may need to be defined as SMTP mail server in some programs. Consult your online help for more information.

- IP Packet Filtering Mgmt
  - Kernel-loaded module scans all IP packets on incoming and outgoing transmissions
  - Operational Filter configuration file located at `/etc/opt/ipf/ipf.conf`
  - Changes to configuration are performed by editing templates located in `/etc/security/tcs`
  - Default templates are `high-ipf.conf` and `low-ipf.conf`
  - Template files can be interface specific - multiple low side networks can be filtered differently depending on site requirements
    - Example interface specific conf file: `hme0-ipf.conf`

- IP Packet Filtering Mgmt (con't)
  - Edit using favorite file editor from a `root` role at `ADMIN_LOW`
  - Rule Set policy "Deny All, Specifically Allow"
  - Services can be allowed or disallowed.
    - comment entries to disallow services
    - uncomment or create rules to allow services
  - To Create a new allowed network service, select a similar rule entry, copy, and edit as necessary
  - For changes to take effect, start TCS **Interface Configuration** tool from the TCS **Admin Tools** Desktop,
    - Select **Save and Exit** from **File** pull down menu
    - IP packet filtering rules will be regenerated in `/etc/opt/ipf/ipf.conf`

- IP Packet Filtering Mgmt (con't)
  - Temporarily allow all network traffic through filters
    - Use to trouble shoot network problems.
    - To open filters, execute this command in `root` role at `ADMIN_LOW`

```
/sbin/ipf -Fa -f /etc/opt/ipf/ipfdown.conf
```

    - To set filters back to normal operation, execute this command in `root` role at `ADMIN_LOW`

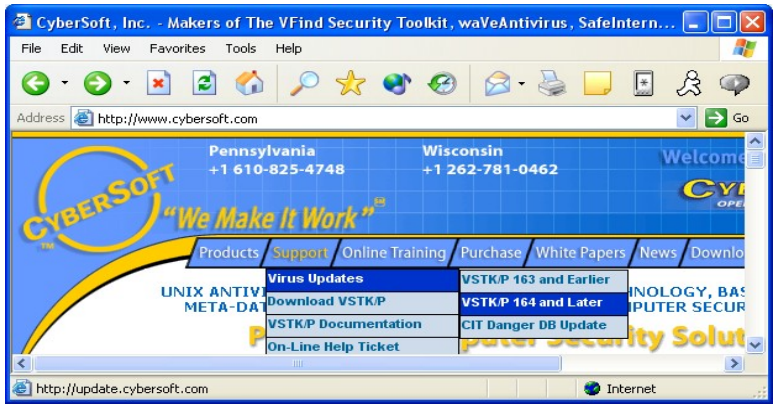
```
/sbin/ipf -Fa -f /etc/opt/ipf/ipf.conf
```

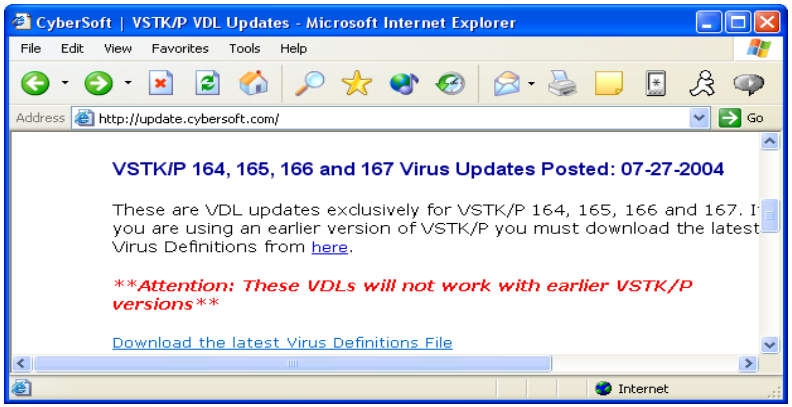
- VFind Virus Scan
  - Overview
  - Setup Virus Definitions
  - Updating Virus Definitions
  - Setup Dirty Word list

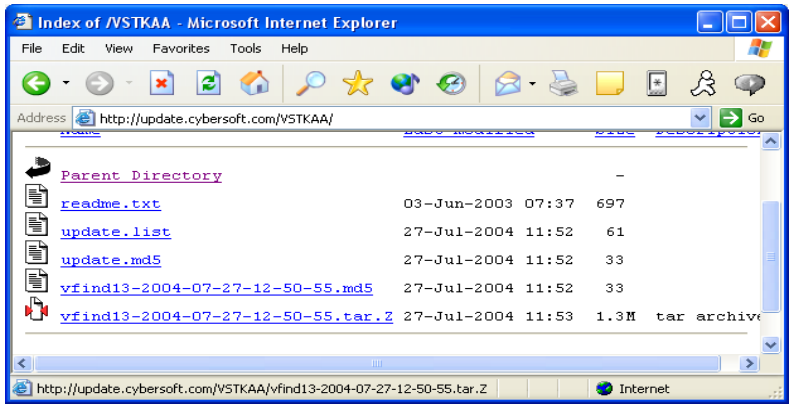
- VFind Virus Scan
  - Overview
    - Full featured virus scanning software from CyberSoft
    - Provides Virus Definition List (vdl) updates
    - Used for Dirty Word Search

- VFind Virus Scan
  - Updating Virus Definitions
    - It is important to periodically update the Virus Definition List (vdl) on your system by downloading a current list from www.cybersoft.com/
    - Select Support→Virus Updates→VSTK/P 164 and Later
    - Download the latest vfind13-<DATE>.tar.Z file and burn it to a cdrom to be used on the TWS.

- VFind Virus Scan
  - Locate the appropriate update file







- VFind Virus Scan
  - Update Virus Definitions
    - Assume the root role at Admin_Low
    - Open the Application Manager
    - Open TCS Admin Tools
    - Double-click the Update Virus Database icon and follow the prompts described in Module Two: TCS Administration Tools

- Printer Management
  - Supports local and remote printers
  - Use **Printer Manager** icon in the **Solaris Management Console** as **`admin`** role in **ADMIN_LOW** workspace
  - Adding a remote printer requires modification to IP Packet Filter template at the level of the printer - uncomment the remote printer rule entry
  - To add local printer, edit /etc/security/device_maps, add a “:” at end of entry by hand using **`root`** role in **ADMIN_LOW** workspace.

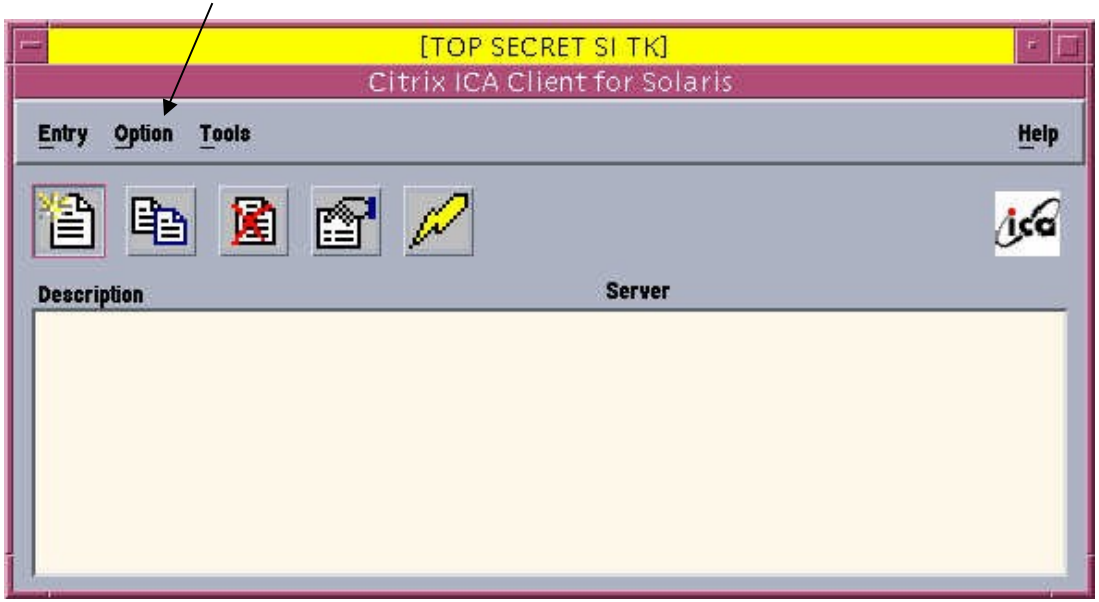
- Miscellaneous Items
  - NFS-mounted filesystems
    - To mount a remote NFS filesytem.
      - » Add IP address for remote system in the following file as `root` role at `ADMIN_LOW`

        `/etc/security/tcs/nfs_ipaddr.conf`
  - Add normal NFS entry to /etc/vfstab
  - Add remote host entry to remote hosts table using TCS **Remote Host** tool.
  - Reboot the system
  - System defaults to “passive” mode for all FTP protocols (XFTP & Netscape)
  - To support active ftp (if remote ftp server does not support passive mode), edit IP Packet filter template file and “uncomment active ftp-data” rule entry.

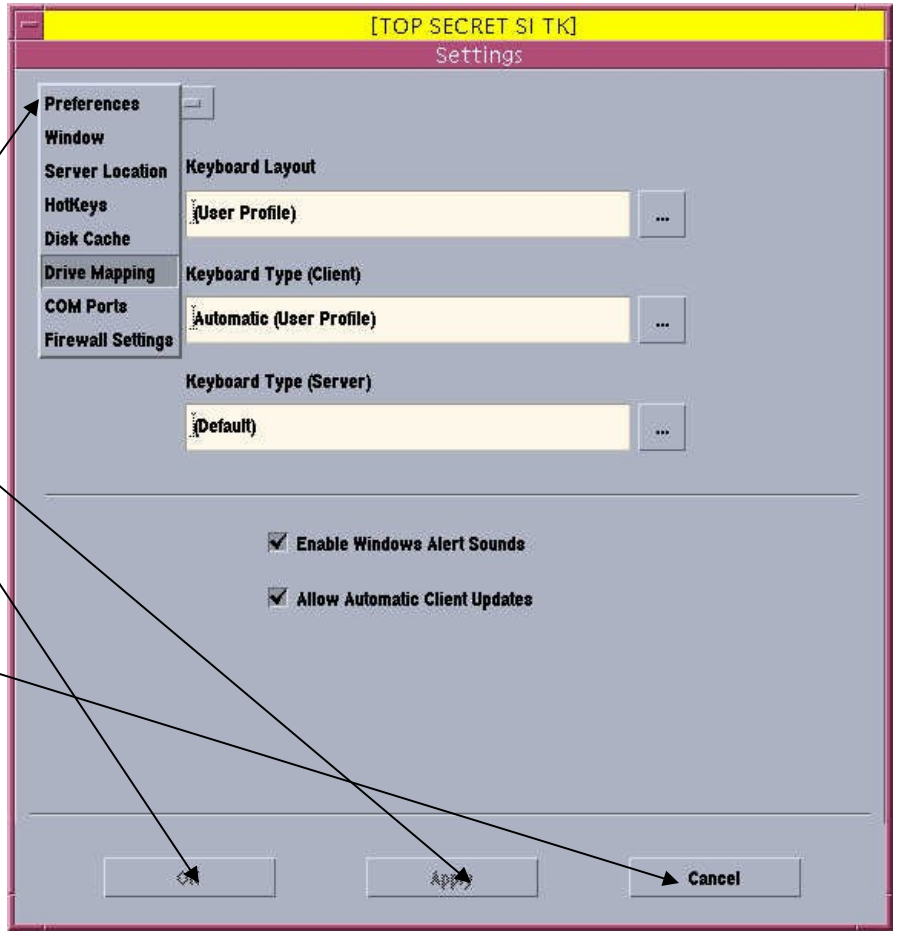
- Citrix Client Management
  - Citrix Client configuration occurs automatically for each level upon users first execution of Citrix Client “Windows”application at each level.
  - Pulls site specific info from a “tar” archive created for the site located in the following file.

    `/etc/security/tcs/mldconfig/ICAClient.tar`
  - mldconfig is a Multi-Level directory containing one level for each site specific configuration set of SLs.

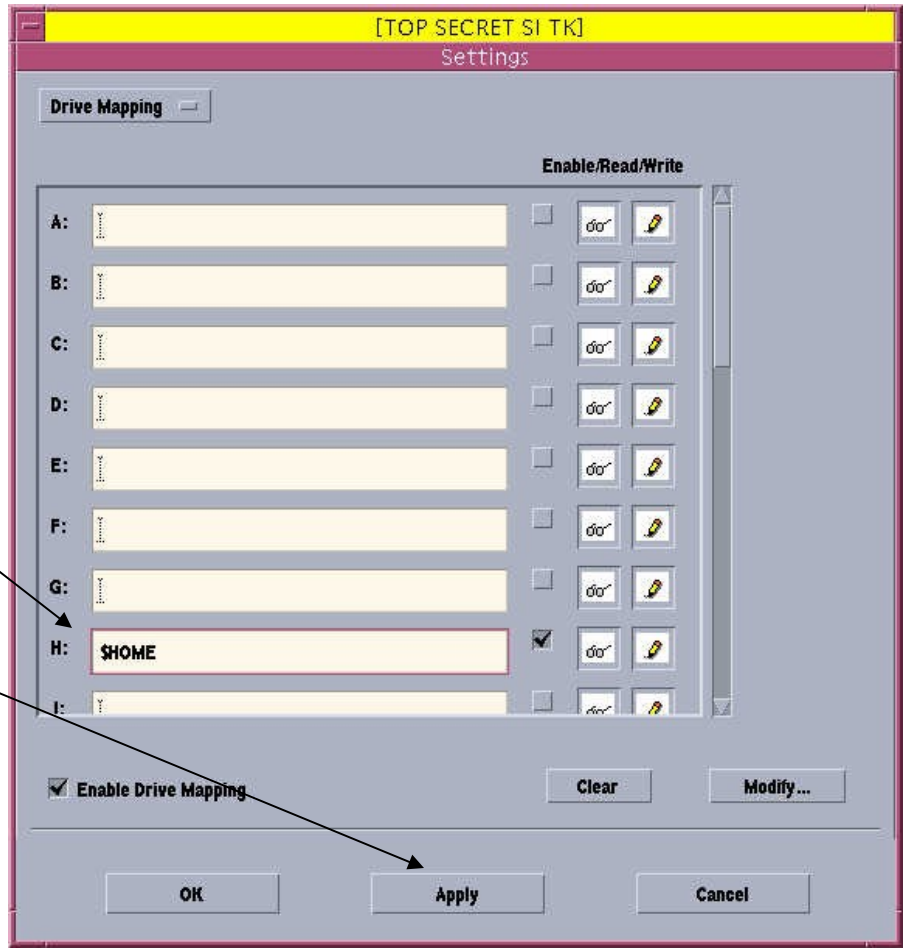
- Creating default client config files
  - Login as “**adminusr**”
  - Launch Citrix Client application “Windows” at each SL you wish to configure for the users.
  - Left single-click on **Options** menu select **Settings**



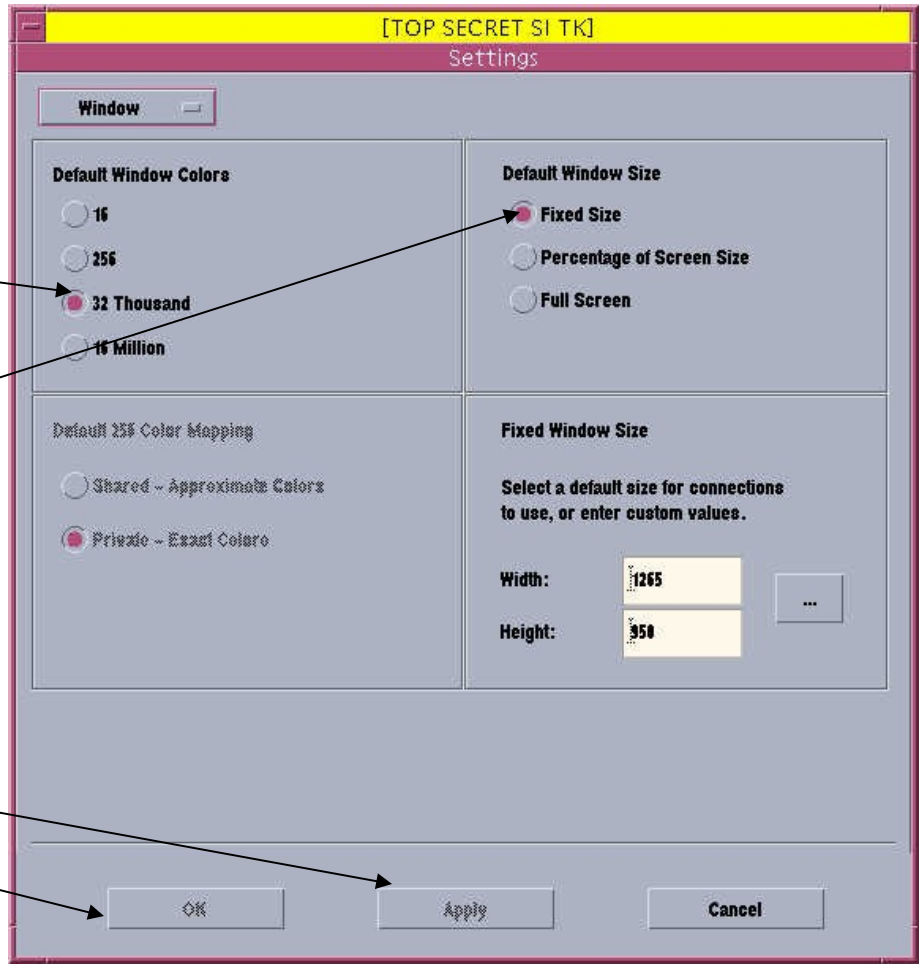
- Create default client config files (con't)
  - From Settings Window
    - Select screens from menu to configure
    - Select **Apply** after each screen is updated
    - Select **OK** when finished to save updates on all screens
    - Select **Cancel** to abort



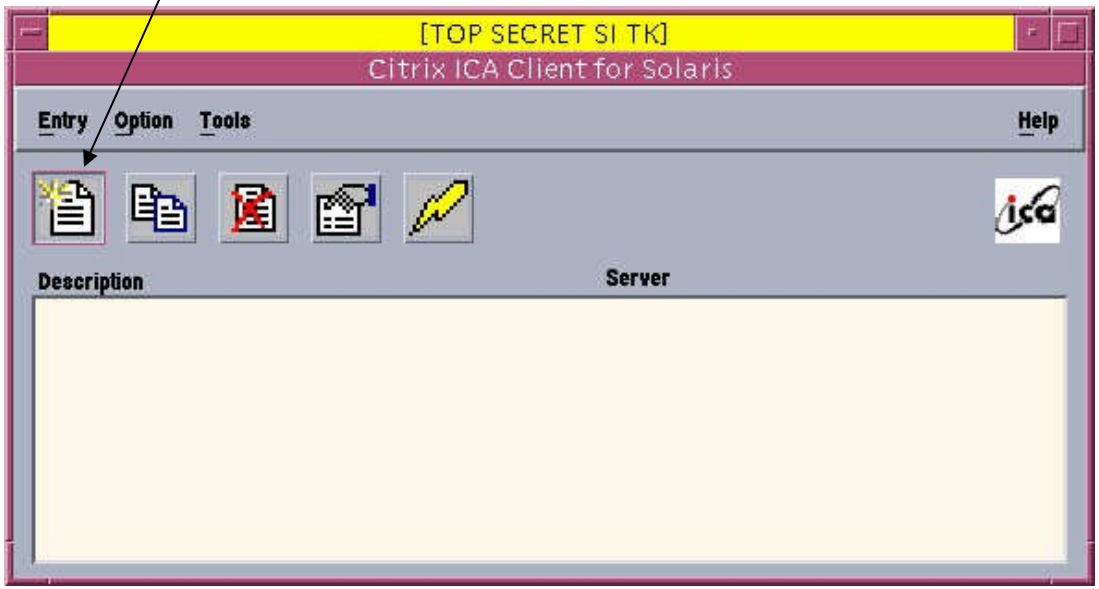
- Create default client config files (con't)
  - Select **Drive Mapping**
    - Set H or a more appropriate drive letter to: $HOME
  - Click **Apply** when finished



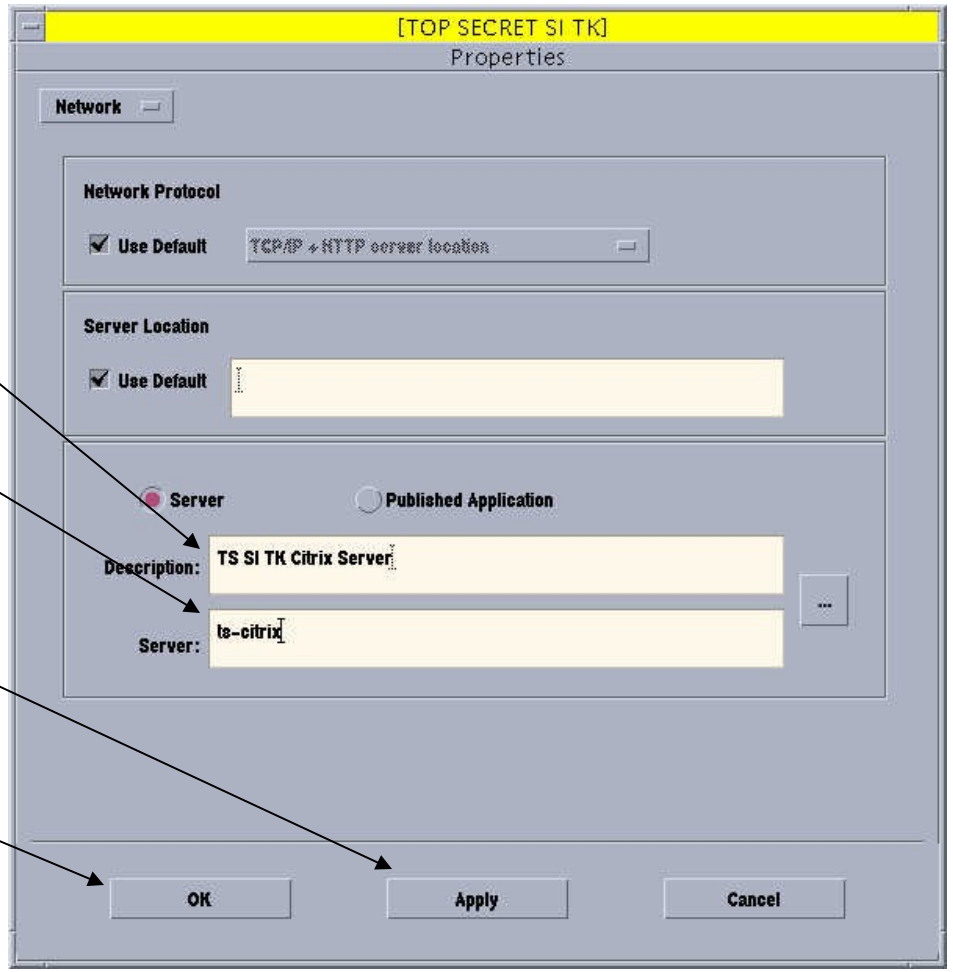
- Create default client config files (con't)
  - Select **Windows** menu
    - 32 Thousand is recommended
    - Select Fixed Size
    - Startup script automatically adjusts the window size
  - Click **Apply** when finished
  - Click **OK** to save and Exit



- Create default client config files (con't)
  - Create Citrix Server Connection
    - Single left-click on New Server Icon



- Create default client config files (con't)
  - Create Citrix Server Connection (con't)
    - Enter server description
    - Enter Server *hostname* or IP address.
    - Press **Apply** when finished
    - Press **OK** to save and Exit



- Create default client config files (con't)
  - Default Citrix Client configuration is stored in a hidden "." dot-prefixed subdirectory of the users multi-level home directory for each SL
  - Hidden subdirectory name is .ICAClient
  - Hidden Subdirectory created as adminusr is then "tar" archived and placed in /etc/security/tcs/mldconfig/ICAClient.tar.
  - ICAClient.tar archive is then used to populate users Citrix client configuration upon initial execution of Citrix Client application "Windows" at the appropriate SL.

- TWS High Security Configuration (HSC)
  - Optional installation parameter
  - Dramatically reduces user desktop actions/icons
  - Can be limited to Windows access only
  - Administrative users must assume roles to perform any administrative function

- Trusted Operating System Overview
  - Roles
  - Profiles
  - DAC
  - MAC
  - Auditing

SecureOffice TWS Administrator

- TWS System Administration Tasks
- Questions?

- Course Overview
  - Module One : Trusted Solaris Review
  - Module Two : TCS Administrator Tools
  - Module Three : TWS Administrator Tools
  - Module Four : TWS System Administration Tasks
  - Module Five: TWS High Security Configuration (optional)